

# to **SECURITY REDUX**

## **How valuable is your data?**

What is everyone after? Why is your data interesting?

## **Mobile devices: the new target**

A look at the top threats you face with a mobile / tablet

## **PC / laptop threats**

New threats that your PC/laptop is subjected to

## **Suite up!**

Security suites are what you need these days...

## **How to stay secure**

Safety tips we should all be aware of...



# KASPERSKY

# Kaspersky Pure

**Total Security**



## For sure shot Home PC safety

**Get the ultimate digital protection for your home PCs with Kaspersky Pure.**

It helps you centrally manage all your home PCs from any PC on the network and offers a [Data Backup and Restore](#) feature to keep you valuable data and files safe.

### **Sure safety Features:**

- Malware and Spam protection
- Enhanced Password Protection
- Advanced Parental Control
- File Shredder
- Data Encryption



A handwritten signature in black ink, appearing to be 'D. D. D.' or similar.

**Available in 1PC, 3PC, 5PC**



# SECURITY REDUX

powered by



# CHAPTERS

SECURITY

MARCH 2012

06

PAGE

## How important is your data

We give you an insight into hacking, hackers and the only thing they are after: your data.

12

PAGE

## Mobiles devices: the new target

Meet the new targets - your mobile and tablets. Take a look at common mobile threats and how they spread

18

PAGE

## PC/laptop threats

It's not just about viruses and malware anymore. We bring a list of the ten new threats which are out there to get you

## CREDITS

The people behind this book

### EDITORIAL

#### Executive Editor

Robert Sovereign-Smith

#### Writers

Meghnail Pagrut & Ankur Mour

#### Copy Editor

Infancia Cardozo

### DESIGN

#### Sr. Creative Director

Jayan K Narayanan

#### Art Director

Anil VK

#### Associate Art Director

PC Anoop & Atul Deshmukh

#### Visualisers

Prasanth TR & Anil T

#### Chief Designer

Baiju N.V

24

PAGE

## Suite up!

Why your anti-virus software is not enough and a guide to selecting the best internet security suite software for you

30

PAGE

## How to stay secure

A collection of safety tips and apps that will keep you one step ahead of the bad guys

### © 9.9 Mediaworx Pvt. Ltd.

Published by 9.9 Mediaworx

No part of this book may be reproduced, stored, or transmitted in any form or by any means without the prior written permission of the publisher.

### March 2012

Free with Digit. If you have paid to buy this Fast Track from any source other than 9.9 Mediaworx Pvt. Ltd., please write to [editor@thinkdigit.com](mailto:editor@thinkdigit.com) with details

### Custom publishing

If you want us to create a customised Fast Track for you in order to demystify technology for your community, employees or students contact [editor@thinkdigit.com](mailto:editor@thinkdigit.com)




COVER DESIGN: ANDOP PC



# Introduction

We live in a world where our laptops and smartphones act as our consorts and hence the responsibility of their security falls squarely on our shoulders. In the ever-changing world of global data communications, inexpensive internet connections and fast-paced software development, security is becoming more and more of an issue. The situation is compounded by the fact that no computer system can ever be completely secure, as hackers and crackers are coming up with new ways to intercept and alter your data – even as you read this. Another mitigating factor to take into account is that the more secure your system is, the more intrusive your security becomes. You need to decide where, in this balancing act, will your system still be usable, and yet be secure for your purposes. In this Fast Track edition, we'll cover this and much, much more.

Dive with us into the fascinating, albeit treacherous, world of hackers and phishers, and discover what they really are after on your device. The rising popularity of mobile devices has caught the attention of attackers. Discover the top ten threats to mobile devices of which you need to be aware. The diversion of the hacker's attention towards your mobile devices, however, has *not* mitigated the risk to your personal computers. Learn how these threats are no longer restricted to viruses and malware anymore. If you were thinking that we're just going to leave you with dire warnings of threat, hold your horses right there. We bring you the best line of defense available in the market – internet security suite software and reasons why they're so much better than plain ol' anti-virus programs. And finally, we'll give you a plethora of safety tips for all your devices and a number of nifty security apps for your iPhones and Android devices. By the time you're done with this edition of the Fast Track, you'll be aware of the ins and outs of computer and mobile security and ways to stay one step ahead of cyber attackers.

So what are you waiting for? Turn the page and kickstart your induction into the world of security. 



# HOW VALUABLE IS YOUR DATA?

We give you an insight into hacking, hackers and the only thing they're after: your data

## What is hacking?

Your computer is like a house and a hacker is someone with pointy metal hats who charge the gate, scale the walls or use stolen keys to get inside to steal your most prized possession or damage your property.

A hacker can mean different things depending on how the term is used. Every programmer dreams of being a hacker. Hackers are programming code jockeys that can throw together bits of miraculous pieces of programming seemingly at will. People who modify computer and other pieces of electronic hardware are also sometimes called hackers.

Being a hacker can also be a bad thing. A hacker or hack can sometimes be someone that has no grace or elegance in his work and throws his projects together haphazardly. Thanks to Hollywood, people think that a hacker is a person who gains illicit access to a computer and steals stuff or breaks into military networks and launches missiles for fun and with no conscience.

Hackers aren't always bad people wanting to ruin your lives. There are White-hat hackers and Black-hat hackers. White-hat hackers are ethical hackers who are computers security experts who attempt to gain access to a computer or network to detect vulnerabilities so that they can be patched. White-hat hackers are also called sneakers, red teams or tiger teams. Black-hat hackers gain unauthorised access to a computer or network with malicious intent. They're also called "crackers". For simplicity we've used the popular mass media definition of hackers interchangeably with crackers.

There's a hierarchy in the hacker community too. An advanced cracker writes his own tools and develops his own break-in mechanisms to gain access to computers. Lower down on the hacker food chain are script kiddies. These electronic intruders use freely distributed tools designed by others to engage in computer vandalism, break-ins, or electronic theft.

## Who are the hackers?

Looking into hackers' minds, you have to be open to the social aspects behind the way they think. Often portrayed as loners, hackers can be socially involved and fit into what is considered "normal" everyday lives. Regardless of the kind of lifestyle lead, every hacker has a knack for solving puzzles and an attitude to push himself to the limit. Their motivations may be different. Some do it for the money, some for a social or political cause and some just do it for the sheer adrenaline rush.

Hackers usually use social engineering to gain most of their knowledge. "Social Engineering" is the act of getting someone to disclose sensitive information through trust. "Brute force", "exploit" and "dictionary attacks" are usually started through the use of software on the hacker's computer.

To avoid detection, he may use proxies or zombie machines so that his location can't be determined.

With the technology and tools available today, hacking has become easier. With the wrong intent, anyone can hack – right from a disgruntled employee to a jilted lover. The disgruntled employee may destroy files or read confidential documents and a jilted lover might reveal intimate details to public. Many high-profile hackers are in their 20s and 30s. However, many are simply teenagers who have access to publicly available hacking tools that can be downloaded easily online.

## What do they want?

A hacker can have many reasons for doing what he does. Here's a list of what hackers are generally after:

- ▶ **Spam:** Most hackers are interested in getting their code onto personal computers so that they can be turned into spam machines. This way they can publicise useless products for which they get paid by the company. If you can hijack thousands of other computers to do the spam-sending, you retain your anonymity and have a spam network that's hard to shut down because each sending machine has to be blocked one at a time.
- ▶ **Corporate data:** Corporate networks are highly protected because they have very sensitive data. A breach in the security can compromise their ability to function. A hacker knows this and hacks into the system to extort or blackmail the company. He can also steal data and sell it in the black market.
- ▶ **Personal computers:** Your PC has a lot more important data than you think. Although personal computers are not prime targets for elite hackers, they still remain an attractive target for the script kiddies. Most often they look for your financial account details to rip you off your money. Some of them might just want to snoop around in your inbox. Others might want to take control of your laptop.
- ▶ **Mobile phones:** Mobile phones are usually hacked to make free calls while the victim is charged for them. However with the new smartphones, your phone can be targeted for your account details, your personal documents, photos etc.
- ▶ **Web servers:** Any web site is hosted on a web server. If the web server is compromised, the hacker can deface the web site to display information of the hacker's choice to the public.

- **Hactivism:** Hactivism is a form of vandalism or electronic civil disobedience with a political agenda. This usually has altruistic motives.

## Hackers you should know!

### Anonymous

Anonymous is a group of hackers that came about in 2008 and grew famous for its hactivism incidents. It has no leader or controlling party and relies on the collective power of its individual participants acting in such a way that the net effect benefits the group.

When the whistle-blowing web site, WikiLeaks came under fire, Anonymous



The Anonymous Group logo

extended its support to WikiLeaks and launched DDoS attacks against Amazon, PayPal, MasterCard, Visa and the Swiss bank PostFinance, in retaliation to perceived anti-WikiLeaks behaviour. Anonymous called it Operation Avenge Assange. On April 2, 2011 Anonymous launched an attack named #opsony on the



A hacked web site

media giant Sony, in retaliation to the legal action it took against George Hotz (or GeoHot), the coder behind a popular tool that allows homebrew software to run on the PlayStation 3. Anonymous claimed the attack to be a success after it took down the PlayStation Network and other related PlayStation web sites.

The group also hacked the Tunisian government web site to support Arab Spring and Department of Justice-managed web sites to retaliate against the shutdown of MegaUpload. Anonymous has been in the news for its hacktivism since the past two years.

### **Jonathan James (c0mrade)**

He was sent to prison for hacking at the age of 16, becoming the first juvenile to be sent to prison for hacking. He targeted high-profile organisations such as the America's Department of Defence. He created a backdoor that enabled him to view sensitive emails and capture employee usernames and passwords. He also cracked into NASA computers, stealing software worth approximately \$1.7 million. He said that he downloaded the code to supplement his studies in C programming but the code wasn't well written and definitely not worth the \$1.7 million. He committed suicide in 2008.

### **Kevin Metnick**

When he was just 12, he used social engineering to bypass the punchcard system used in the Los Angeles bus system. Later he used social engi-

neering as his primary method of obtaining information, including user names and passwords and modem phone numbers. He was convicted for hacking into multiple systems of the Digital Equipment Corporation to view Virtual Memory System (VMS) code which cost it \$160,000. At the time of his arrest, he was the most-wanted computer criminal in the United States. Kevin also admitted to stealing software from Motorola, Novell, Fujitsu, Sun Microsystems and other compa-



Hacking: He's doing it right!

nies, in addition to altering the computer systems of the University of Southern California.

After serving his sentence, he decided to mend his ways. He started Mitnick Security Consulting and is now turning a profit as a white hat.

### **Stephen Wozniak (Woz)**


A white-hat hacker, he was also called the other Steve of Apple. Along with Steve Jobs he co-founded Apple Computers. He started hacking by making blue

boxes – devices that bypass telephone-switching mechanisms to make free long-distance calls. He and Jobs researched frequencies, then built and sold blue boxes to their classmates in college. He came up with the preliminary Mac, and Jobs had the bright idea of selling the computer as a fully assembled PC board; thus creating one of the most important breakthroughs in computing technology. He no longer works for Apple and devotes his time and money to philanthropy.



The "other" Steve

### **Ankit Fadia**

India's very own ethical hacker who shot to fame after authoring *The Unofficial Guide to Ethical Hacking* at the age of 15. He's an independent computer security consultant and also advises the government on matters of cyber security. Faida has also led several investigations pertaining to national security and cyber terrorism. He's currently pursuing his Bachelors in Computer Science with specialisation in Information Security at Stanford University, USA. 



# MOBILE DEVICES, THE NEW TARGET

Meet the new targets – mobiles and tablets. Take a look at common mobile threats and ways in which they spread

**M**obile malware is clearly on the rise, as attackers experiment with new business models by targeting mobile phones. Take for instance the DroidDream malware that was found in the Android Market a year ago. Till a few years ago, a security

threat to mobiles meant data theft but mobile payment has changed that; your money is at risk too. The value of mobile payment transactions is projected to reach almost \$630 billion by 2014 which makes it an attractive target for attackers.

The risk of identity theft has always lingered over mobile devices. Since all your personal data is stored in your phone, a simple attack on your phone can enable an attacker to know your passwords, phone numbers and address.

## How safe is your OS?

Although developers are trying to create secure operating systems for mobiles, a fully secure OS still remains an utopian concept. After learning from security flaws in PCs, Android and iOS have each taken an innovative approach to securing both, the operating system and application distribution process.

### iOS

Apple's iOS security model runs each third-party application in an isolated environment so that the application may only access its own data and permitted system resources. All third-party applications are granted access to the same data and capabilities on the device with the exception of a few, such as location data and push notifications, which require a user to opt in for each application.

When it comes to app distribution, all apps submitted by developers go through a manual review process with restrictions based on policies regarding issues such as data collection, API usage, content appropriateness and user interface guideline compliance.

### Android

Android has an operating system security model that supports its open application distribution model. In this security model, an application's capabilities are gated by permissions that the app declares when it's installed



Mobiles aren't safe anymore

and can't be changed at a later time. When installing an app, users are presented with the list of permissions requested by the app and can determine whether the permissions are appropriate for the functionality of the app. Permissions allow apps to access specific data and capabilities on a device, including location, contacts, SMS messaging, identity information, and the ability to access the internet. If an app's permissions seem overreaching, a user may choose not to install the app or may identify it as suspicious.



The App Store logo

The Android Market has a more community-based approach than Apple's App Store. Some security checks are performed when apps are submitted to the market, but it's expected that the community as a whole will participate in identifying malicious or otherwise undesirable apps. This allows Android developers to update their apps much more quickly than with Apple's curated model.

## Threats to your mobile device

We can split mobile threats into four major categories – application-based threats, web-based threats, network-based threats and physical threats. Most of these threats are also common to computers. We've further split them into sub-categories.

1. **Application-based threats:** Just like the malicious software on PCs, apps present many security issues on mobile devices. These can be categorised in four ways:
  - a. **Spyware:** This is designed to collect or use data without a user's knowledge or approval. The most commonly targeted data is phone call history, text messages, location, browser history, contact list, email, and camera pictures. Spyware can be used to gather data from a particular group of people; eg. parents monitoring their child's phone. It can also be untargeted, designed to gather data about a large group of people. Targeted spyware apps are typically installed by somebody who has physical access to a victim's mobile device and there are a lot of commercial surveillance apps that can do this. Targeted spyware apps often have very legitimate use cases and are not always used maliciously.

- b. Malware:** Malware is software designed to engage in malicious behaviour on a device. They can perform actions like sending text messages to your contact list without your knowledge or give the attacker complete control over your phone. They're also used to steal personal and financial data which can be used for identity theft or financial fraud. In the last year, threats due to malware increased from 34 per cent to 48 per cent.
- c. Vulnerable applications:** Sometimes a developer isn't careful while designing his app and there might be certain loopholes in the app which can be exploited for malicious purposes. They can often allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, automatically download additional apps or otherwise engage in undesirable behaviour.  
If an app is transmitting data over an unencrypted Wi-Fi network using HTTP (rather than [HTTPS](#)), the data can be easily sniffed using freely-available software. Vulnerable apps are typically fixed by an update from the developer.
- d. Privacy threats:** Some applications gather more sensitive information than required to function posing a threat to your private information. A gaming application which looks into your contacts and your email is a fine example of this. Although not malicious, they're a cause for concern.

## 2. Web-based threats:

- a. Phishing scams:** These scams are designed to dupe ignorant internet users and get login information. Everyone reading this has got at least one mail asking them for their username and password probably in exchange for continuing to be able to use Facebook/Gmail which "is shutting down all fake accounts". There are phishing sites (fake web sites) designed to look like a bank's web site and trick users into giving their login information. Most of you might not have fallen into this trap but as per statistics, approximately 1 in 20 users will click on a phishing link every year on Android devices. Always remember that a legitimate web service will never ask you mail your password. Also, always check the URL of the web site before logging in.
- b. Drive-by downloads:** These are downloads that happen without your knowledge. They automatically begin downloading an app when you visit a web page.

- c. **Browser exploits:** They're designed to take advantage of vulnerabilities in a web browser or software that can be launched via a web browser such as a Flash player, PDF reader or image viewer. Simply by visiting a web page, an unsuspecting user can trigger a browser exploit that can install malware or perform other actions on a device. Such attacks are a significant concern on devices where apps can be downloaded outside of official markets because malware distributed through web sites can evade the greater scrutiny that markets provide

### 3. Network threats:

- a. **Wi-Fi sniffing:** This can compromise the data transferred over a Wi-Fi network. If the app or the webpage doesn't use proper security by not encrypting data, it may be easily intercepted by anyone listening across an unsecured local wireless network. While the tools for Wi-Fi sniffing facilitate targeted rather than broad-based attacks, the increased use of free Wi-Fi in airports, cafes and other public places has increased the likelihood that Wi-Fi traffic, including account information, can be intercepted.
- b. **Network exploits:** The flaws in your software on your mobile operating system can be exploited by

attackers using Bluetooth or Wi-Fi. Network exploits often don't require any user intervention, making them especially dangerous when used to automatically propagate malware.



A single "s" can mean the difference between secure and insecure

- 4. **Physical threats:** Since the mobile is a portable device, it can be easily lost or stolen. Besides the financial loss, there's the loss of all private and sensitive data.

## How they spread

The most common technique hackers use is called Repackaging. This tactic involves taking a legitimate application like Gmail/Gtalk and modifying it to include the malicious code. The attacker then hosts this infected app on his web site. This way when a user installs the infected app, the code runs in the background so the user has no idea that his device is infected. The

most frequently repackaged apps are games and legitimate apps downloaded from “free” web sites. That’s why you should always download apps from official web sites. Sometimes repackaged apps are hosted in the Android Market/AppStore. They look similar to the original apps however they differ in their permissions. The repackaged apps ask for more permissions than required. Although Google and Apple are trying hard to remove such apps, it never hurts to be careful.

Even if you install a legitimate app, you can be the victim of an Update Attack. Malware writers first create a malware-free app and when they have a large user base, the creator updates the application with a malicious version. Because many users have their devices set to automatically update applications or will manually update whenever a new version is available, the update attack technique minimises the amount of time the malware is in the market before it’s installed on a large number of devices.

Phew! That’s a quite a lot of malware. In the coming chapters we’ll give you tips on how to stay protected. 



The internet is a double-edged sword; it can just as easily harm you



# PC/LAPTOP THREATS

It's not just about viruses and malware anymore. Here's a list of the ten new threats out to get you

### Internet worms

Worms are often used to infect a large number of broadband-connected computers with remote-control software. An internet worm works differently than a virus. It won't attach itself to different programs to be harmful but will produce a precise copy of itself. Worms often infect computers by exploiting bugs in legitimate software. Worms spread via networks and consume bandwidth. If you've ever wondered why your network is slow,

your computer could be infected by a worm. They'll have many malicious effects such as causing a server to crash, render a user's files unusable or create a backdoor to track a computer.

## Rootkits

A Rootkit is often a collection of programs which are hidden deep into your system. They enable administrator-level access to a computer or computer network. An attacker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password, and then hides its presence on a PC. The first rootkit was documented in 1990s on Sun and Linux operating systems but today rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network. It creates a backdoor and allows the hacker to send spam email or use the target PC to perform a denial-of-service (DoS) attack on servers. Detecting it is tough as it will conceal its presence in a computer. One means to detect it is by running a virus scanner when it's not running because a rootkit masks itself as a useful utility and the anti-virus can't detect it. If a rootkit is detected, however, the only sure way to get rid of it is to completely erase the computer's hard drive and reinstall the operating system. This is because anti-virus and malware removal tools running on an untrusted system may be ineffective against well-written rootkits.

## Zombies

A zombie computer, or "drone," is a computer that has been secretly compromised by hacking tools which allow a third-party to control the computer and its resources remotely. When a trojan has infected a user's laptop, it can open a "backdoor" to permit hackers to use the infected computer for malicious purpose without the owner's knowledge. The user generally remains unaware that his computer has been taken over – he



Worms – a pain in the behind since time immemorial

can still use it, though it might slow down considerably. Communication between the hacker and the computer travels through back channels of the targeted system, keeping these processes hidden from the owner.

The hacker will sell the target laptop access to others and others can use it for their own purpose. If a spammer has gained access to the target PC, he can use it to send spam. It allows spammers to avoid detection and presumably reduces their bandwidth costs. Since the owners of zombies pay for their own bandwidth, zombies have been used extensively to send e-mail spam; as of 2005, an estimated 50–80 per cent of all spam worldwide was sent by zombie computers. The user might find that his Internet Service Provider (ISP) has cancelled his service, or even that he's under investigation for criminal activity. Meanwhile, the cracker shrugs off the loss of one of his zombies because he has more.

## Browser hijacker

A browser hijacker or hijackware is a type of malware program that alters your computer's browser settings so that you're redirected to web sites you had no intention of visiting. Most of the time, it will modify your homepage, error page or search page. It can disable your internet option therefore you can't change the homepage to the default homepage. Furthermore, the browser hijacker will edit the registry therefore it can run each time you restart Windows.

This is generally done by crackers to redirect traffic to their web site or their client's web site which pays for the traffic it generates. More aggressive versions can add pornographic bookmarks or pop-ups which can be a nightmare for your corporate life. Browser hijackers are installed as a part of "freeware" installations and the hijackware is disguised as an add-on to it. It's mentioned in the user agreement but the problem is that users typically ignore the End user Licence Agreement (EULA). A browser hijacker may also be installed without user permission, as the result of an infected e-mail, a file share, or a drive-by download. It's advisable to read the user agreement, be careful what freeware you download off the internet and not click on links in suspicious emails or on social networks.

## Phishing

The first documented use of the word "phishing" was in 1996. Most people believe it originated as an alternative spelling of "fishing," as in "to fish for information". Phishing email messages, web sites and phone calls are mainly designed to steal money. For example, if a phisher wants

your bank account's username and password, he creates an exact copy of the bank's web site, he then finds out your email address and mails you threatening that your account will be closed if you don't send fill in your login details.

## Spam

Spam used to be junk or bulk email sent by the spammer to various recipients aimed at advertising, scamming or sending viruses. But over the years, it has developed and needs to be defined in a new way: any kind of unwanted information sent to you by an unverified source is spam.

Besides the usual emails, there are many fake sites popping up. They claim that you can "Earn \$8769/month right from your home". Sounds too good to be true, right? That's because it's spam. These links take you to fake web sites and the moment you enter your email address you become a part of a huge spam list and this is how you get 100s of spam mails a day. Even worse, the hacker can gain your personal information like your phone number and home address which can be used for identity theft. If you come across such links always remember "there is no free lunch".

Are your friends posting links on Facebook saying "OMG I can't believe this..."? If yes, they're victims of Clickjacking. This is how it works: when your friend clicks a link on Facebook saying "Best Justin Bieber video ever" s/he is asked to fill an online survey or subjected to some kind of ad. At the same time, the embedded code spreads via their profiles making it seem like they liked it and posted it on everyone's wall. This problem was prominent a few months ago but Facebook has tried to control it and also filed lawsuits against the perpetrators.

## Spyware

Spyware is a type of malicious software employed by hackers and advertisers to achieve information about you without your knowledge. Spyware creators go to great lengths to ensure that their software remains undetected. It differs from a virus because a virus is a piece of code designed to replicate itself as many times as possible, spreading from one host computer to other computers connected to it and damages your operating system. A spyware is a code made just to track your activities. The damage it does is more of a by-product of its main mission, which is to serve you targeted advertisements or make your browser display certain sites or search results or even send your personal data to the attacker.

Most often you're infected because of your own actions. Do you tend to click on links offering you "99% discount" on flights? If yes, you should scan your computer for spyware. These applications often use trickery to get you to install them, from fake system alert messages to buttons that say "cancel" when they really install spyware. Most spyware run as an application in the background as soon as you start your computer up, hogging RAM and processor power. They make your web browser slow by constantly opening pop-up ads. Sometimes they control your search results rendering your search engine useless. A very malicious spyware can record the words you type, your web browsing history, passwords and other private information.



Phishing for information

## Mousetrapping

Don't you feel annoyed when you want to leave a web site and can't? This is often referred to as mousetrapping. Mousetrapping is a technique used to trap an unwilling visitor at an offending web site in order to gain maximum benefit from the one-time visit. Hackers copy code of legitimate web sites and add a bit of code that would redirect them to a completely different web site. Since the code mirrors the original web site they also end up in search engines thus a surfer can't tell if a link is bogus or not until he or she clicks on it. Thus you might click to get a great discount deal and might end up opening a porn site.

The attacker knows that the unwilling visitor will try to close the web site as soon as they see an offensive web site therefore they incorporate additional redirect code that prevents leaving, while using the visitor's clicks to generate revenue. This way when you click on "Back" or "Close", it begins a loop opening one offensive site or advertisement after another, popping up banner after banner in a cascade of windows. Although, this is fairly harmless, it can cause pretty embarrassing moments for you.

## Network threats

Many people feel that their home network is at a low risk for attack. Especially in India, people think that no one bothers to hack networks but if you have a Wireless Access Point on your network you're at risk. If the ISP


detects and tracks the illegal activity to your address, then you'll have a lot of questions to answer besides paying the hefty bill.

The biggest threat to a wireless network is if it's unprotected, usually because users are ignorant or because of the "chalta hai" attitude. However, an unprotected network can be a nightmare for your security because someone can clearly see your unprotected network on their scan, connect to it and access the host computer with no password or identification at all.

Denial-of-service attacks is another major risk. It can happen even if your network is protected. A DoS attack is almost just as it sounds. Your connection to the internet can be severed by being overrun by thousands of constant transmissions. A DoS attack can completely disable your network and your PC.

## Hidden data

Have you every thought about what other data you inadvertently share with someone when you exchange documents? Even if you're just sharing MS Office documents, you may discover that you're inadvertently supplying more information than you realise. This extra data is called Metadata. It contains your name, your company name, the name of the server or hard disk that you stored it on, document revisions, comments etc. Used for a variety of legitimate purposes, it adds functionality to the editing, viewing, filing and retrieving capabilities of Microsoft Office.

But in the wrong hands it can compromise your security and you might end up revealing more to someone than intended; e.g. negative comments that you put in a presentation can be retrieved by your client. In order to avoid these consequences, familiarise yourself with the types of metadata contained in your documents and take steps to remove it whenever necessary. Some basic metadata can be accessed through the Microsoft Office interface but you'll need a binary file editor to access the other metadata. 



In the wrong hands your sensitive data can be used against you



# SUITE UP!

Why your anti-virus software isn't enough. Plus a guide to selecting internet security suite

**T**he year 2011 was remarkable in many ways. For people who make internet security their top priority, it will be remembered as a year that was full of events that exposed our internet security vulnerabilities and made us wonder how safe we are using the web.

With each wave of cyber-attack, users woke up to find that their personal pics and identities were at risk from all angles – via social media accounts, email accounts, game providers and mobile phones. But hang on! The cyber-attacks weren't just restricted to private individuals – even governments, large companies and global defense companies were facing the firing squad.

## Why do you need to take security seriously?

Let's take a look at the five most publicised cyber-attacks that grabbed headlines last year.

1. In September of 2011, two men were arrested by British police in connection with cyber-attacks conducted by the Anonymous and LulzSec hacker groups. The arrests followed a series of hacks and DNS attacks on U.K. and U.S. businesses, government bodies and law enforcement agencies. In the last year, Anonymous took on Sony, child porn sites, the city of Orlando, BART, Cox Communications, SOPA and more.
2. Millions of Sony PlayStations were hacked. Although credit card information was encrypted, personal information was not. Sony sent out 77 million emails to account holders whose information may have been compromised. As a safety precaution, Sony was forced to implement a password change campaign and 12 months of identity theft protection offered via Affinion International Limited.
3. Sites such as “IsAnyoneUp” became quite a rage. This particular site in question came under the radar, for posting nude pictures (often submitted by an ex-boyfriend or girlfriend) next to a screenshot image of their Facebook profile.
4. Japan’s biggest defense contractor, Mitsubishi Heavy Industries, was attacked by malware, which affected their computers and network servers in 10 facilities. It was reported that sensitive data, including information about jet fighter planes and nuclear power plant plans, could have been compromised. In addition, the group called “Nitro” by Symantec targeted nearly 30 chemical firms and defense industry companies.
5. Christopher Chaney was arrested for hacking into celebrity email accounts and phones. The investigation, called “Operation Hackerazzi,” identified more than 50 victims, including celebrities Scarlett Johansson, Christina Aguilera, Lady Gaga and Miley Cyrus.



Sony officials bowing their heads in shame !



The Anonymous strikes back !

If you still feel you don’t need protection, it’s time to wake up and take notice. Everyone – from

private internet-users to defense companies – need internet security and Internet security suites is the way to go. Internet security suites are comprehensive security that not only provides anti-virus protection but also anti-spam, antispyware, privacy, anti-phishing and internet search protection.

## Why internet security suites?

One trillion dollars – that's the rough estimate cybercrime is expected to extort this year from governments, businesses and individuals. Yet every day more and more businesses, government agencies and entertainment companies are making the leap to online access at a record pace. And who can blame them? We love the internet. It makes our lives easier and provides instant gratification; however, it also provides access to our computers and – even more critical – personal information.

As security threats have grown to encompass more than viruses, security experts have adopted the term malware to describe all malicious code. Combating this stew of invaders requires in-depth defense – multiple barriers between the malware and your system. This is exactly what internet security suites software provide.

## Internet security suites vs. Anti-virus software

Anti-virus software provides an essential layer of protection from a multitude of virus, trojan, worm, spyware, adware, dialer, keylogger and rootkit infections. Traditionally, anti-virus programs just detected viruses but most current anti-viruses have reasonably good detection rates of all forms of malware. But this still ain't enough!

Anti-virus programs don't detect all forms of malware. According to one of the most trusted independent anti-virus testing bodies, AV-Test.org, more than one million unique malware samples are created a month, and presently the total amount of unique samples in their malware collection exceeds 22 million. With the huge increase in malware, anti-virus software cannot keep up with detecting all of it. So you can see how tough it is to detect all of it.

What makes an internet security suite different from traditional anti-virus software is that it also includes other layers of protection, including anti-spam, anti-spyware, parental controls, privacy protection and much more to protect you and your PC or laptop from all angles. Many of the top security suites also include helpful extras such as secure password managers, file shredders, full screen modes and web site advisors.

## A word of caution

The market is filled with all sorts of computer security programs. Research before deciding on a security program. There's plenty of security software out there that can do more harm than good to your computer. Rest assured though that there are more legitimate security programs out there than illegitimate ones.

## Internet security suite: What to look for

The best internet security suite can protect your computer and personal information from threats coming from all pathways – via the internet, connected drives, email attachments, corrupted video files, malicious applications, unsecured wireless connections and USB-connected devices. They will even protect your computer from your kids. Here are the criteria, which you can use to tell a good internet security suite from a great one:

- **Internet protection**

When it comes to deciding between two internet security suites, always opt for the one that has a proven track record for providing consistent, reliable and proactive internet security. The best-rated suites are rated so high because of their ability to combat known and emergent threats as well as detecting suspiciously behaving applications. You should be on the lookout for security suites that provide not just anti-virus protection but also privacy protection, social network protection, spam filters, web site ratings and more.

- **Security features**

The best Windows internet security suites go beyond basic virus protection to provide complete security through additional security features including parental controls, password managers, game modes, laptop tools and safe browsing. Another very important parameter is the ability to customise these settings. Though most users like their security software to run unobtrusively in the background using default settings, others want to fine-tune the software to react in a specific manner to particular web sites or users. You should choose the software based on your personal preference.

- **Help and support**

The security provider should offer adequate support through online



Protect your data

documentation, community forums, FAQs, help files and beyond. They also should provide free telephone, email and chat support via a helpful and knowledgeable support team. The top internet security selections provide support during extended support hours, continuous software updates and timely threat information.

## How to test different internet security software suites?

On any given day, one vendor may be a little quicker on the draw to prevent a virus than others. That makes evaluating the strength of a particular anti-malware or anti-spam product very difficult. You can test each security suite based upon factors that affect you directly:

- ▶ Ease of installation
- ▶ Ease of use
- ▶ Notification capabilities
- ▶ Updating time
- ▶ Quality of the interface

When you're testing new software suites, you should check how long the machines take to boot up, once you have successfully installed the software product on your notebook. You can then compare that figure to the time it had taken the machine to boot up without a security suite installed. After each test, you can restore the notebook back to its pretesting condition using any "Backup & Recovery Suite" – this ensures that each product is installed under the exact same conditions, with the same software configuration. During testing, you should also keep a lookout for tell-tale signs of poor performance, such as high processor utilisation and slow system boots. Another important thing to keep in mind is the overall responsiveness of the interface. Finally, beware of the suites which are overly intrusive and get in the way of effectively using your PC by, for example, bombarding you with messages and warnings.



The most popular security suite


## 2012 suites: Faster, slimmer, more effective

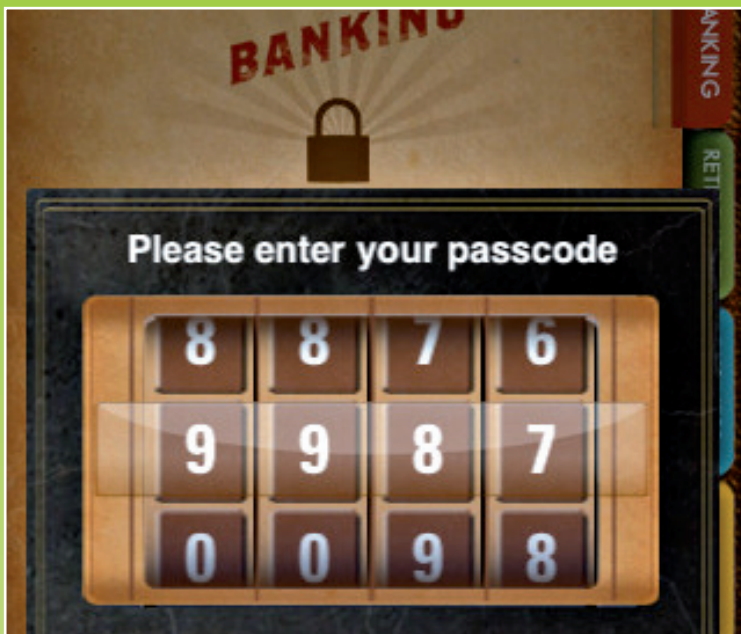
Security Software Suites have evolved over the last few years. As malware has become more sophisticated, so have security suites. One interesting trend is the inclusion of digital sandboxes, which work by executing unknown applications in protected memory to detect any malicious behavior before allowing the application to access the system. Another innovation is application-stamping, where known good applications are whitelisted, allowing the anti-malware software/firewall to skip rescanning the applications whenever they are launched. That helps to speed up application launches and minimise the CPU cycles needed by the security software.

Another emerging trend in fighting malware is the use of cloud computing: The security suite on your PC enlists the



The most popular anti-virus software

power of the software maker's massive online systems to help detect threats. Some anti-malware packages use cloud computing to supplement other detection technology. What's more, security software vendors are becoming more proactive about protecting your PC, especially when it comes to updating signatures. Many of the products here check for new signatures several times a day, which is helpful for combating zero-day threats from new exploits. 



# HOW TO STAY SECURE

A collection of safety tips and apps  
that will keep you one step ahead of the  
bad guys

**T**ill now, we've told you about the different threats to your computers, laptops, tablets and smartphones and how to keep a lookout for them. Keeping the dire prophecies of doom aside for a bit, we'll now tackle the different ways you can protect

your computer system against the dangers of the digital community. In the end, we'll give you a round-up of the best security apps out there for your iPhone and Android device.

## Personal computer/laptop security

Admit it – you can't possibly imagine your life without your favorite gadget. Whether you own a laptop or a tablet or a smartphone; it's an inclusive element of your life. They're your own consorts and it is up to you to ensure their security.

- **Have strong passwords**

A good password manager can help generate incomprehensible passwords, store them in its database, and decode them locally, only on your machine, when it needs to enter them into the web site. Each site will have a different password, you'll have no idea what any of them are, and all you'll have to do is remember the one master password you set for it.

- **Encrypt your data**

If someone should get your laptop and gain access to your files, encryption can give you another layer of protection. With the Windows operating system, you can choose to encrypt files and folders. Then, even if someone gains access to an important file, they can't decrypt it and see your information. You could use open-source tools like TrueCrypt or the built-in BitLocker that's available in some Windows versions.

- **Use a screen guard**

These guards help prevent someone from seeing your screen – even if he or she peeks over your shoulder. They can be very useful if you need to work on sensitive information in a public place, and they're especially helpful when you're traveling or need to work in a crowded area.

- **Limited obtain**

Making it possible for every person to view your laptop/PC can be something that is the most important source of threats. Your computer data might be corrupted and also stolen; settings



Protect your computer – Protect yourself!

could be improved on purpose pertaining to malevolent applications and several programs can be installed that will be a traveler with you as long as you're however unacquainted with the item. Hence you should consider creating individual accounts on your system, and granting limited but specific access to each of these users.

- **Security suites software**

Internet security suites software are comprehensive security software that not only provides antivirus protection but also anti-spam, antispyware, privacy, anti-phishing and internet search protection. As security threats have grown to encompass more than viruses, security experts have adopted the term malware to describe all malicious code. Combating this stew of invaders requires defense in depth--multiple barriers between the malware and your system. This is exactly what Internet security suites software provides.

- **Firewall**

A solid firewall will help you stop intruders from accessing your system. You keep your internet link to the outside world but the outside world can't view you unless you want them to. With a firewall in place you will still have typical email access, but chat and other interactive programs will require you to take an extra step to grant access before you can use them. A firewall is powerful but unobtrusive, just like a deadbolt lock inside a door.

- **Choice, assembly and updating problems**

Selecting the most appropriate system for one's technique is on the list of essentials of your safeguarding process. There's no sense in spending tons of money on a very strong but incompatible application, as it can affect various other software programs, thereby bringing down the overall performance of your system. After you've decided on the correct system, make sure that you install it in the appropriate way with the recommended settings. Don't forget to allow automatic updates.

- **Other tips**

- ▶ A BIOS password is something laptop users could consider as an extra security measure, because it's not easy to bypass it on laptops
- ▶ LAlarm is a Windows-only laptop alarm security software that helps

you set up various alarms in order to prevent laptop theft. It has theft alarm, perimeter alarm, inattention alarm, battery alarm, disk alarm, data destruction and recovery facility and much more.

- ▶ LaptopLock is a data protection tool for your laptop that can safeguard your data and also delete it if you lose the laptop. In fact, it can also encrypt data, launch programs and do much more when your laptop is reported stolen on their site.
- ▶ Yawcam, as the name indicates, is a webcam software that could turn your webcam into a motion-sensing tool which could then be used to keep an eye on people trying to access your laptop when you're not around.
- ▶ Prey is a nifty software that's multi-platform and provides a number of features to track your laptop or phone when it is lost. It uses GPS or auto-connects to a wireless connection when you send a signal remotely through SMS or internet, and then you could use it find your device's location, lock it down or monitor the activities of the person using it.



Software tools to protect your computer

## Tablet/mobile security

When all you need to do to make a payment is a physical tap, it might seem awfully convenient but it sure will be ripe for exploitation. In February 2012, the Google Wallet's PIN system was cracked twice over a span of two days, compromised by both rooted and un-rooted Android phones.

The first attack came when security firm “zvelo” discovered that a rooted Galaxy Nexus stores PINs on the device rather than the secure NFC chip, thus making the phone vulnerable to brute-force attacks. If the phone falls into the wrong hands, your PIN and whatever other passwords saved in the device can easily be identified. But that's the risk you take when you root your phone.

However, the second security breach discovered a day later, showed that even unrooted phones were in danger. This time, the method was foolproof. All the user had to do to enable Google Wallet was reset the data under the app settings, which would prompt him to enter a new PIN without asking for the old PIN. After wiping the old data, this new bypass allowed the user to link the account to a Google Prepaid Card, which then provided access to all previously available funds. The phone was as good as a cashier not asking to see your ID when you pay with credit card.

The safest way for Google to save your PIN is to secure it via the NFC chip, which requires action from your banks. While the two parties sort out new terms of service, there are several things you can do to keep your phone safe. This is what we're going to tell you about in this chapter.

## **Step 1: Enable password protection**

The easiest way to secure your smartphone is with a password, making it the best place to start. We're going to concentrate on the more popular mobile operating systems and how their password (or password-like) security works.

### **► iOS**

It's very easy to set a passcode on iOS, but it's no more secure than a PIN number. Fortunately, if you're running iOS4 or higher you can set a password instead. To set your iOS password or passcode, open the Settings app. From there, go to `General > Passcode Lock > Turn it on` and enter your new password or passcode.

### **► Android**

Android's additional security comes in the form of a swipe pattern (unless you're running Android 2.2 Froyo, in which case you can also set a PIN or password). To set one, go to `Settings > Security > Change Unlock Pattern > Require Pattern`. You'll be able to enter a swipe pattern. Coming up with something easy won't do much to help, so figure out a complex swipe pattern you can remember.

### **► Windows Phone 7**

In Windows Phone 7, you're able to set a lock screen password. To do this, flick left to go to `Settings > Lock & Wallpaper > turn on Password`. You'll be prompted to enter a new password twice. Do this and press "Done" to save your changes.

## ► BlackBerry

To set a password, simply go to **Options > Security Options > General Settings > Password to Enabled**. You can also decide how long the device sits idle before it locks up. If you're using a device like a Pearl that has a multi-tap keyboard, try to come up with a password that only requires one tap on each key.

## Step 2: Enable remote wipe

If you've added a passcode/password/pattern/p-whatever to your smartphone and you're still paranoid, it may be time to explore remote wipe. Remote wipe does what the name implies: it remotely wipes the data on your phone and restores it to the factory settings.

## ► iOS

Setting up remote wipe on an iOS device is easy, but only if you have all the right ingredients. You need a paid MobileMe account that's currently active on your iOS device if you're running a version of iOS prior to 4.2. You also need to enable push and Find My iPhone. Once Find My iPhone is enabled, you'll be able to log into MobileMe and wipe your iPhone.

## ► Android

Remote wipe is a built-in possibility on an Android device, but it requires Android 2.2. Additionally, you need to have Exchange set up. In the event Exchange is set up, a remote wipe can only be performed by an administrator. However you might be better off, adding remote wipe via a security app. We're going to tell you about some cool apps, in the next section.

## ► Windows

Windows Phone 7 can easily be wiped using Outlook Web Access. We're not going to go into the details here, but there are a number of cool videos on the internet to help you do so. Check out <http://www.youtube.com/watch?v=NoL-5d-kaNs>

## ► BlackBerry

Firstly the user would need to download and install the BlackBerry Protect application on



Setting up your unique swipe pattern

their BlackBerry smartphone. This nifty application allows you to lock your BlackBerry smartphone, set a password, set a 'lost and found' screen, 'view current location feature', and you can even use the Remote Wipe feature to delete all the information off the device, including the data stored on the device and on the Micro-SD card.

Apart from these there are a number of other steps you can take. The top antivirus providers offer software specifically designed to protect handheld devices. It's worth your while to review all of your options and choose a solution that best fits your needs. Check out the section below to know the best security options in the business. Also keep in mind that when you step outside the closed environment of a trusted app store, you're exposing yourself to the malware that these sources screen out. Stick to trusted app stores.

## Security apps for your iPhone

Some of them are free but most will cost you. We suggest shelling out a few bucks in the best interest of your iPhone. Here are eight security apps for the iPhone, which every owner should take a look at.

- **Find My iPhone**

This app, designed by Apple, can be used for both your iPhone and iPad. If you misplace your iPhone, iPad, iPod Touch or Mac, the Find My iPhone app will let you use another iOS device to find it and protect your data. Simply install this free app on another iOS device, open it, and sign in with your Apple ID. Find My iPhone will help you locate your missing device on a map. You can then choose to display a message or play a sound, remotely lock your device or erase your data on it.

- **Security Organizer**

This neat little paid app has you covered for all your memory lapses. It will automatic log out if the device is left unattended, copy and paste long passwords and IDs directly from apps and automatically delete information after failed login attempts.

- **SNAP**

Snap is a useful security tool to discover open ports as well as a fun way to probe public networks to see who else is on with you. Snap quickly scans the network around your phone and discovers nearby servers, routers and even other iPhones! When Snap finds a device, it shows you

the manufacturer of the device, any name information it could discover from the device, as well as the device's MAC and IP addresses.

- **Intego VirusBarrier**

Mac security firm, Intego's VirusBarrier application scans the iPhone, iPad and iPod Touch for malicious content. Unlike comparable Android products, the VirusBarrier application scans only files downloaded onto the device, such as email attachments and files downloaded from the web. The sandbox technology used in iOS prevents VirusBarrier from being able to see what other applications are doing.

- **Lookout Mobile Security**

The iPhone offering from Lookout Mobile Security is different from its Android, BlackBerry and Windows Mobile counterparts. While Lookout still hasn't added an anti-malware component to the iOS application, it does warn about unsecured networks. This iPhone application checks for the latest version of the iOS, whether the device has been jailbroken, backs up data, allows users to track lost or stolen devices, remotely wipes data on lost devices and warns about location-tracking services.

- **GadgetTrak**

GadgetTrak can take a picture of the person using the device and email it to the registered address on file, letting users find out who may have their phone. The web-based service tricks thieves into sending location data to GadgetTrak servers to identify where an iPhone is. The application can also be turned on remotely, so it doesn't need to be running until the phone is actually lost.

- **Firewall iP**

Firewall iP provides firewall features such as blocking outgoing connections on the jailbroken iPhone, iPod Touch or iPad. Similar to the Little Snitch personal firewall for the Mac OS X, Firewall iP allows users to create policies, block connections for applications when on the cellular network, and block certain types of content.

- **Cisco AnyConnect / Junos Pulse**

iOS devices come with a built-in VPN client that can be configured to use with the Cisco AnyConnect or Junos Pulse from Juniper Networks. Junos

Pulse for iOS allows users to establish secure connections over Secure Sockets Layer VPNs to corporate applications.

## Security apps for your Android device

Android devices are able to support a wide range of security functionality that runs in the background, from automated backups to virus scanning. What's more, the most essential security precautions for your Android device, like password-protecting the device itself and setting it to auto-lock after a specified period of time don't require an app; both of those features can be accessed within "Settings -> Location & Security."

And with an ever-growing number of apps available, what follows below certainly isn't an exhaustive list, but it's intended to give you a good sense of some of the options available when seeking further protection for your Android smartphone -- and for the data that resides on it.

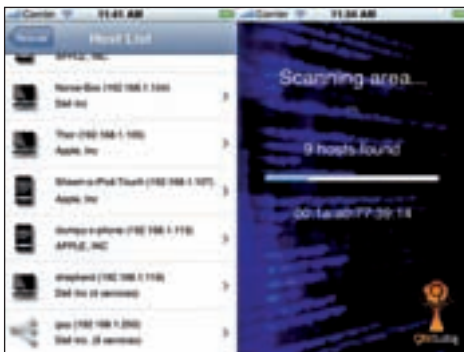
### • Lookout Mobile Security

Lookout Mobile Security helps you protect your phone and includes antivirus, backup and Find My Phone. The app allows you to block

viruses, malware and spyware by scanning every app you download. Backup allows you to back up your contacts and photos, as well as restore data to a new or existing phone. Find My Phone can help you pinpoint your phone on a map, activate a loud alarm to find



Locate your lost iPhone

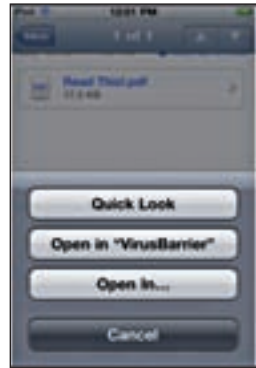


SNAP it all !

your phone, and if necessary remotely wipe your data if your phone is lost or stolen.

- **AVG Antivirus**

Another big name in computer security, AVG Antivirus Free scans your apps, settings, media and phone contents in search of suspicious files. Have a text message with a shady-looking link attached? Run the scanner to see if it's a possible threat to your phone's security. Features that the creators will add in the future include the ability to lock apps and back up data.



Check out those attachments

- **NetQin Anti-virus**

Although NetQin Anti-virus provides features similar to those of Lookout, its focus seems to be on helping you recover your lost or stolen phone. With NetQin's Anti-lost feature, you can track your phone, erase its contents, lock it down to prevent "illegal use," and have your phone emit an alarm that sounds similar to a loud police siren.



The most popular security app

- **McAfee WaveSecure**

McAfee WaveSecure is the mobile security service that protects data on your phone, ensures privacy in the event of theft and enhances the possibility of recovering your phone. The app lets you remotely lock down your device and wipe out important data if necessary, backup and restore data, as well as track and locate your handset.



Trick or Thief !

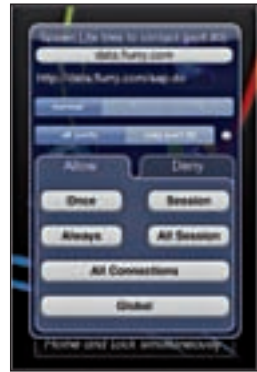
- **Webroot Mobile Security**

This app brings Webroot's powerful

online security to your Android device. This lightweight security app eliminates malicious applications, blocks harmful web sites, and protects your privacy if your device is lost or stolen.

- **Norton Mobile Security**

Symantec's Norton Mobile Security (beta) allows you to remotely lock and wipe your phone by text message, so that whoever finds it can't immediately go on a shopping spree. You can even lock down the SIM card so that a thief can't swap it out to another phone. Beyond that, Norton permits you to block calls and text messages, as well as to scan your phone for malware.



Block outgoing connections


- **MindWallet**

MindWallet allows you to store a wide variety of sensitive information that is accessible with one master password. Features include military grade 128-bit AES encryption, inactivity timeout, backup and restore, and search. MindWallet also includes predefined templates or allows you to create custom templates for your personal needs.



Establish secure connections

- **mSecure**


mSecure is a password and data manager that offers a convenient and secure solution to store information on Android devices. Use mSecure to safely store sensitive and important information as mSecure uses an industry-proven data encryption method so your information is safe guarded should your device be misplaced or stolen. 

# SECURITY SNAPSHOT

To give our readers a better understanding of Kaspersky's products, their philosophy, and their expectations and predictions for the year ahead, we sat down with Mr. Harry Cheung, Managing Director, Kaspersky Lab – APAC, in a brief question-answer session. Here are some excerpts from the interview:




Mr. Harry Cheung, Managing Director  
Kaspersky Lab – APAC

 **One thing about Kaspersky software that's unique, and one thing that will never change?**

 At Kaspersky Lab, we have earned quite a reputation for rapid and comprehensive malware detection. Traditionally, we always have small disk and memory usage, and we have further improved on this feature in our new offering using a mix of cloud and on-the-PC protection. The Hybrid protection model works optimally to ensure protection against known as well as unknown threats. Because of its advanced threat detection capabilities, Kaspersky Security Network (KSN) immediately knows of attempts to infect PCs. As a result, in less than 40 seconds, millions of KSN users are alerted and protected.


We have been technology leaders from day one, and that is our forte. It will continue to be so.

## **In the latest edition of Kaspersky security software, how is malware detected?**

 In the current edition, we use Hybrid technology, which is a mix of cloud and on-the-PC protection. The cloud technology (Kaspersky Security Network) has updated details on the threats, and also employs a strong Heuristic methodology to ensure protection against unknown malware. Once the user installs, activates and updates our product, the modules on his PC take care of offline protection; when the user gets online, KSN protects it from all internet-based threats.

The new 2012 versions feature integrated, world-class protection technologies designed to combat even the most complex of threats. At the same time, these products are now simpler and more user-friendly than ever before.

## **How do you see the malware landscape shaping up in 2012? Any trends or predictions?**

 We expect to see the following events and trends this year:

- Rise of Android malware
- Data theft and location-tracking
- Increased targetted attacks especially towards enterprises & government institutions
- Widespread attacks on online banking systems.


## **Top global destinations from where malware originates?**

 India has emerged as one of the top countries generating spam in 2011. Last year, the number of infected computers used for sending spam increased in Asia and Latin America regions. One of the reasons is that although internet communications are quickly developing, the level of security threats awareness among population is very low in these countries. Moreover, India doesn't have anti-spam legislation.

## **Do you plan to equip upcoming tablets and smartphones with pre-loaded Kaspersky Mobile Security suite?**

 We will unveil our tailored security solution for Android-based tablets – Kaspersky Tablet Security on 28 February at Mobile World Congress 2012, in Barcelona, Spain. The product includes cloud technology support for anti-virus technologies, web security and anti-theft protection. It is a specialized security solution that ensures both, protection against malicious and fraudulent software, and the inviolability of personal data in case of loss or theft of a device.

## **Help us understand Kaspersky's India operations.**

 We have two offices: Hyderabad and Mumbai with dedicated teams for Retail and Enterprise business. We have established ourselves as a leading player in the country, thanks to our partner network and team. ◀

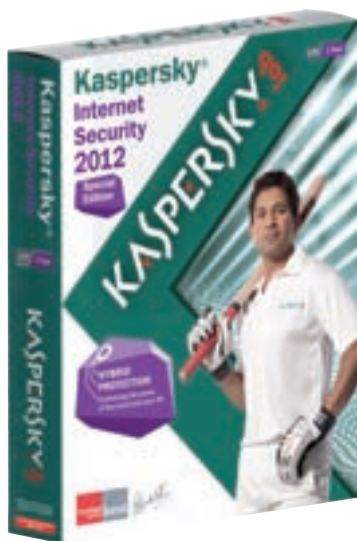
# KASPERSKY LAB PRODUCTS: THE ULTIMATE DIGITAL PROTECTION

Over 300 million people worldwide are protected by Kaspersky Lab products and technologies. Kaspersky Lab's corporate client-base exceeds 200,000 companies located around the globe, ranging from small and medium-sized businesses, all the way up to large governmental and commercial organizations. What makes Kaspersky Lab products the first choices of preference for our customers globally? Let's find out more about these multi-award winning products and the expert anti-malware technology that drives them.

## Kaspersky Internet Security 2012

### Hybrid protection

You, your private data and PC are completely protected as you work, bank, shop and play online. Watch out for the Sachin Tendulkar special edition packaging!



### Key Features

- ▶ **Improved Kaspersky URL Advisor:** Marks web links with a color-coded tag that shows their danger level
- ▶ **Kaspersky File Advisor:**
- ▶ **Improved System Watcher**

- ▶ **Safe Run Mode**
- ▶ **Two-way personal firewall**
- ▶ **Improved Anti-Phishing and AntiSpam technology**
- ▶ **Improved Parental Control**
- ▶ **Completely redesigned interface New!**

### Pricing and availability

Kaspersky Internet Security 2012 is available at ₹899 and ₹1499 for 1 user and 3 users, respectively in all computer stores across the country.

## Kaspersky Mobile Security 9

### The best protection for your smartphone

In the event that a smartphone is lost, the data in its memory also remains protected. Kaspersky Mobile Security runs on smartphones with an Internet connection and any one of the following operating systems:

- Android: 1.6-2.3
- BlackBerry: 4.5-6.0
- Symbian (Nokia): Symbian^3 or Series 60 9.1, 9.2, 9.3, 9.4
- Windows Mobile: 5.0-6.5

#### ▶ **Privacy Protection**

With the touch of a button you can mark a contact as 'private', meaning that no trace of them will appear in contact lists, SMSs and call logs. Other people using your mobile will only see what you want them to see.



- Supports contacts from both the onboard memory and SIM cards
- Password protected

#### ▶ **Anti-Theft**

Remotely Block your phone if it is lost or stolen or Wipe your data..

Set a prearranged message that will be displayed on the screen if the smartphone is blocked, allowing any law-abiding citizen that finds your smartphone to return it to you.

You can locate your smartphone using GPS Find. Just send an SMS with the appropriate password to the missing device and you will receive a link to Google Maps showing the exact location of the device.

The first thing a thief normally does is remove your smartphone's SIM card. If the SIM is replaced, SIM Watch will

immediately block the device and send you an email with the new number.

#### ► **Encryption**

Give sensitive information on your phone an extra level of security. Password-protect & encrypt folders on your smartphone (even if it is located on a memory card).

#### ► **Anti-Spam**

Anti-Spam can run in whitelist mode (only accepting calls and messages from specified contacts) or in blacklist mode (accepting calls and messages from all numbers except those on the list).

#### ► **Parental Control**

Block outgoing calls or SMSes to undesirable numbers. GPS Find allows you to track your child's location.

#### ► **Anti-Malware Protection and Firewall**

Real-time protection from malware, on-demand or scheduled antivirus scans, automatic updates over-the-air and blocking of dangerous network connections in line with a predefined security level.

### **Pricing and availability**

Kaspersky Mobile Security is available at ₹599 in mobile stores across the country.

## **Kaspersky PURE – Total Security**

### **Total protection for life online**

It gives you the peace of mind of knowing your digital life is safe, your

PC is in tip-top condition, your most valuable information is secure and your family is protected.

## **Key Features**

Kaspersky PURE is designed with the home user in mind, combining simple installation and management with advanced features and functionality.

#### ► **Malware and Spam protection**

► **Centralized Management** of tasks, reports, updates and more from any PC on your network

#### ► **Enhanced Password Protection**

► **Advanced Parental Control** protects your family with unique features to monitor your kids' Internet access, PC and application use and communications... including social networks.



- ▶ **File Shredder** uses multi-pass technology to make deleted data unrestorable
- ▶ **Data Backup & Restore**
- ▶ **Data Encryption**

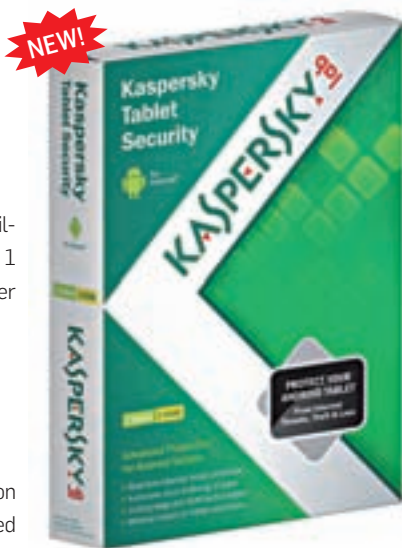
### Pricing and availability

Kaspersky PURE - Total Security is available at ₹1995, ₹3495 and ₹4695 for 1 user, 3 users and 5 users in all computer stores across the country.

### Kaspersky Tablet Security

#### Advanced protection for Android tablets

- ▶ Real-time, cloud-enabled protection
- ▶ Virus-scanning of apps downloaded from the marketplace
- ▶ **Advanced anti-theft protection**
  - FIND missing tablet with GPS, GSM or Wi-Fi and Google Maps
  - Personal, web-based control center for Anti-Theft functions
  - Remotely activates: Lock, Wipe, Find and Mugshot
- ▶ **Web protection & management**
  - Detect and block fraudulent links
  - Review logs of recent activities, such as commands activated and their status and results
- ▶ Small, frequent updates that won't slow you down ◀



## About Kaspersky Lab

*Kaspersky Lab is the largest antivirus company in Europe. It delivers some of the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. The company is ranked among the world's top four vendors of security solutions for endpoint users. Kaspersky Lab products provide superior detection rates and one of the industry's fastest outbreak response times for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. Learn more at [www.kaspersky.co.in](http://www.kaspersky.co.in). For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, visit [www.securelist.com](http://www.securelist.com).*

# KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS

## Be ready for what's next

**K**aspersky Lab's newest innovation – the Kaspersky Endpoint Security 8 suite helps you fully protect and control changing IT environments.

### Solution Offerings:

- ▶ **Work Space Security:** Protection for workstations, laptops and smartphones.
- ▶ **Business Space Security:** All of the above plus protection of file servers.
- ▶ **Enterprise Space Security:** All of the above plus protection of mail and groupware servers.
- ▶ **Hosted Security Services:** Hosted protection for business-critical processes such as email and Internet use.
- ▶ **Total Space Security:** Multi-layer protection for workstations, laptops, smartphones, mail servers, groupware servers and Internet gateways.

### Key highlights:

- ▶ **Application Startup Control:** Provides administrators with the ability to grant, block and audit application launches.
- ▶ **Administrator-based Whitelisting:** Provides administratively assigned and cloud-assisted predefined cat-

egories of whitelisting rules for application startup control.

- ▶ **Application Privilege Control:** Applies restrictions to various actions of applications in the operating system as well as rights to access computer resources.
- ▶ **Vulnerability Scanning:** Prevents potential exploits by identifying system weak points, missing patches and neglected application and OS updates.
- ▶ **Device Control:** Allows granular control of external device operations – enforces usage policies and reduces the risk of data loss.
- ▶ **Web Control and Content Filtering:** Monitoring and filtering users' browser activities by category, content and data type, regardless of workstation location.

### Pricing and availability

Can be purchased as part of the Kaspersky Open Space Security product line. To help you choose the most suitable product, consult a sales manager with one of Kaspersky Lab's partners. The list of Kaspersky Lab partners is available at [www.kaspersky.com/buyoffline](http://www.kaspersky.com/buyoffline).

Pricing varies as per the total number of nodes that require protection ◀

# KASPERSKY LAB'S TIPS ON SAFE SOCIAL NETWORKING

## **Social networking cybercrime**

Cybercriminals use social networking sites, like Twitter, Facebook, Bebo, MySpace or LinkedIn to distribute malicious code or befriend unsuspecting users to steal their personal information. Follow the five simple steps below to keep yourself protected.

1. Post minimum personal information
2. Only post information or photos that you are happy for anyone to see
3. Be wary of strangers
4. Use strong passwords or ideally use a password manager
5. Use Internet Security Software and keep it up to date

## **Other social media risks**

Avoid opening any links that come into your e-mail inbox from a social networking site. Even if it is a social network that you are a member of, it is far safer to directly log on to that site and check your messages from there.

Internet fraudsters typically use genuine logos, good business style

and may even spoof the header and sent-from of the e-mail to make it look legitimate. But phishing scams are the bait used to try and lure customers into clicking on the link included in the e-mail. The link takes the user directly to the specially constructed site.

By not clicking on links that may be fake, you are one step closer to protecting yourself online. This approach, applied alongside installing Internet Security, will keep you and your internet accessible devices as safe as possible.

There is always the risk that even private information that is restricted could be exposed, so it really is important that you don't post anything that you wouldn't want the public to see. Also, be cautious when deciding which applications (apps) to enable. Check your settings so you know what information the applications will be able to access – and to make sure you do not unwittingly reveal private information. ◀

# Kaspersky Mobile Security 9

# KASPERSKY

[www.kaspersky.co.in](http://www.kaspersky.co.in)

## Smart protection for smartphones



**Kaspersky Mobile Security 9** has sharp features that make your smartphone theft-proof, trespass-proof and intrusion-proof. Get smart today.

#### Features:

- Secures your phone against mobile malware
- Makes your private contacts invisible
- Helps locate your lost smartphone\*
- Blocks or wipes data on your stolen phone
- Keeps your most private data encrypted
- Prevents unwanted calls and SMSes

\*Only on GPS enabled smartphones

**FAXTEL**  
*Just a little ahead of time*

**National distributor (Mobile Security Solutions): Faxtel System (India) Pvt. Ltd.**

- Mumbai (022 2611 3055)
- Delhi (011 4132 4829)
- Bengaluru (080 2530 1403)
- Chennai (044 2815 8471)
- Hyderabad (040 4200 6320)

**Channel partner enquiries are welcome.**

**E-mail [saleskms@faxtelindia.com](mailto:saleskms@faxtelindia.com)/call 080 2530 1740/96861 91142**



# Kaspersky Lab becomes a Leader in the Magic Quadrant

Kaspersky Lab has been named a **'Leader'** in the **Magic Quadrant for Endpoint Protection Platforms**.

The Magic Quadrant is the most influential benchmark for companies seeking to evaluate vendors and products in the IT security industry based on criteria in two categories: completeness of vision and ability to execute. It plays a very important role in purchase decisions of enterprises on a global scale.

**Kaspersky Endpoint Security 8's** rapid and comprehensive malware detection, its manageability, advanced HIPS features and broad endpoint platform support are factors that have played a role in its new position on the quadrant.

Reach us at: [india-sales@kaspersky.com](mailto:india-sales@kaspersky.com)

**KASPERSKY** <sup>lab</sup>

**Kaspersky for Business**